Research on SDN-based IoT Security Architecture Model

Shiji Zheng
Department of Electronic and Information Technology, Jiangmen Polytechnic
Jiangmen, China
engii@163.com

***Abstract*---With the rapid development of the Internet of Things(IoT), the traditional IoT architecture model no longer meets its security requirements. Determining how to effectively discover and eliminate the security threats in the Internet of Things has become an urgent problem that needs to be solved. The idea that Software Defined Network(SDN) separates the control plane and the data forwarding plane gives an new and excellent resolution to the security problems of IoT. The research applies SDN technology into the IoT and builds an architecture model aiming to improve the security of the IoT. Through simulation experiments, the architecture model can effectively improve the security of the IoT.**

Keywords*---*Internet of Things; SDN; self-similarity; security

Ⅰ. INTRODUCTION

In recent years, with the development of network communication technology and the popularity of various smart devices, the application of the IoT has become extensive. IoT has been considered as a great opportunity in the field of information technology. However, with the rapid development of the IoT, its huge and complex architecture and massive data transmission are being threatened severely, which is one of the bottlenecks restricting the development of the IoT.

Although the IoT architecture model is complex and the data transmission is huge, its security protection is weak, especially its perception layer. It is generally operated in an unattended environment with low performance, limited resources, and traditional network security. Traditional security protection is no longer applicable. New revolutions and methods that are compatible with the Internet of Things should be applied. This paper proposes an SDN-based IoT Security Architecture Model. It adds a gateway layer which is used in data security detection and control in the traditional IoT architecture, and implements the pre-position of IoT security policy deployment. Flexible configuration and centralized management of security resources and security rules, starting from the source of IoT data, effectively improve the security of the Internet of Things.

Ⅱ. Traditional Internet of Things Architecture Model

The traditional internet of things architecture model is generally divided into three layers, perception layer, transport layer and application layer [1], as shown in Figure 1.

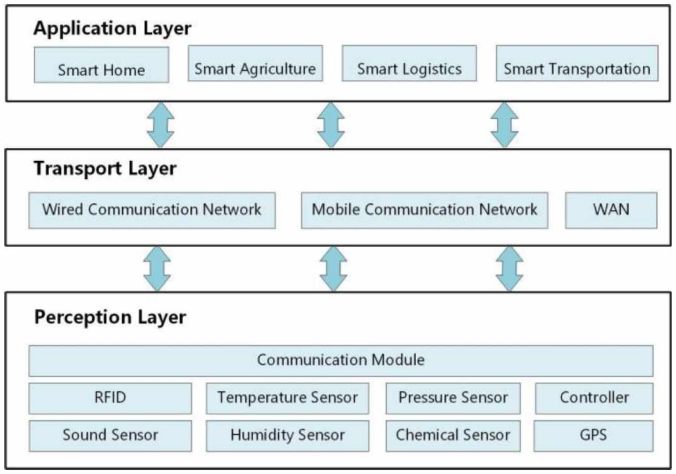

Fig.1. Traditional Internet of Things Architecture Model

The perception layer obtains, collects and identifies the data of physical, chemical and environmental variables through pressure sensors, temperature sensors, sound sensors and other sensing devices functioning the data acquisition and location [2].

Perception layer is the basic unit of the Internet of

Things. Sensors are ubiquitous. The security of perception layer is very important, but it has been always neglected. It is reflected in the following aspects:

(1) The type, quantity and dispersion of sensing devices are often not included in the security management of the whole system , and are vulnerable to attack;

(2) Operating system or software is out of date; the vulnerabilities are not repaired in time;

(3) Because of limited computing and storage resources, traditional protection measures such as anti-virus and new security technologies cannot be applied.

The transport layer is to transmit data from the perception layer. The data collected by the perception layer is usually transmitted to the application layer by means of mobile, wired and wireless communication technologies and WAN communication systems.

The application layer is the embodiment of the practical application of the IoT. According to the specific needs, it analyses and processes the data from the transport layer, makes correct decisions, controls and provides feedback; it provides intelligent applications and services to meet the actual needs, such as smart city, smart transportation, smart logistics, smart home, etc.

III. SDN Technology

Nowadays, in the transmission network, the hardware and software are closely combined, which controls the data by receiving, storing and forwarding together. Therefore, the efficiency of data transmission highly depends on the hardware performance and software algorithm of the device.

SDN is the future direction of network development. It is a new virtual network architecture model designed to deal with the problem of heavy load and lack of flexibility of existing network architecture model. It originated from a research project of Stanford University in 2006 [3]. The basic idea of SDN is to separate the control function and data forwarding function and give the network programmable ability [4]. The centralized management and dynamic configuration of SDN are designed to improve the management and controlling capability and utilization of the whole network. The structure of SDN is shown in Figure 2.

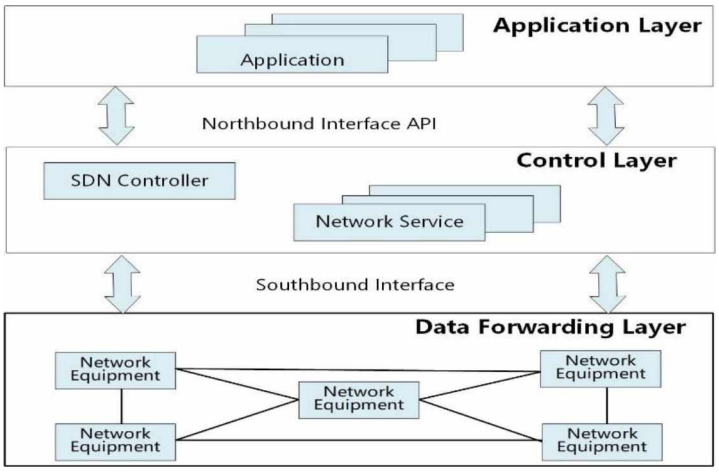

Fig.2. Structure of SDN

The structure of SDN can be divided into application layer, control layer and data forwarding layer [5]. The top layer is the application layer, which is composed of APIs with different functions to meet the specific business needs of users. The middle one is the control layer, the core part of SDN. It is composed of SDN controller. It maintains the data exchange table in SDN and manages the operation of the whole SDN network. The northbound interface protocol interacts with the application layer, and the southbound interface protocol interacts with the data forwarding layer[6]. It functions the download of FlowTable and the monitoring of the whole network information. The bottom layer is data forwarding layer, composed of SDN switches and other network devices. Data forwarding is implemented according to the rules issued by the controller.

OpenFlow is one of the core technologies of SDN [7,8]. Through OpenFlow, the controlling and forwarding of data are separated. FlowTable of OpenFlow is composed of flow items of priority sequence , which can match and query the field of data packet quickly. When the data packet enters the OpenFlow of SDN-supported switch, it queries the FlowTable content to get the number of the destination port. OpenFlow enables to define special rules in order to allow regular traffic to choose its path freely as needed. The interaction between the gateway and the controller must run on the secure channel through the OpenFlow protocol.

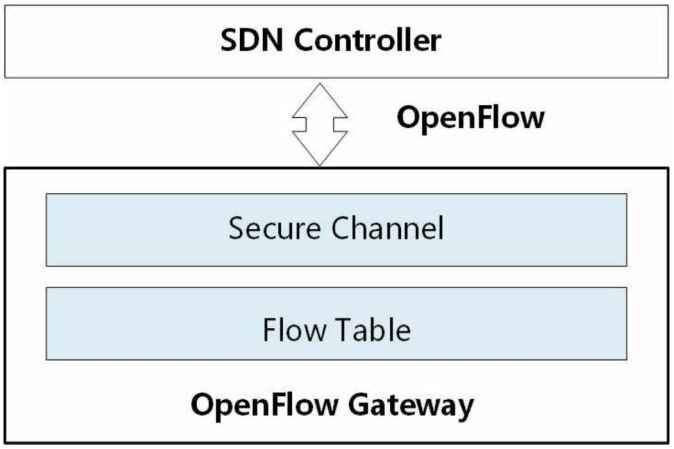

Fig.3. OpenFlow composition diagram

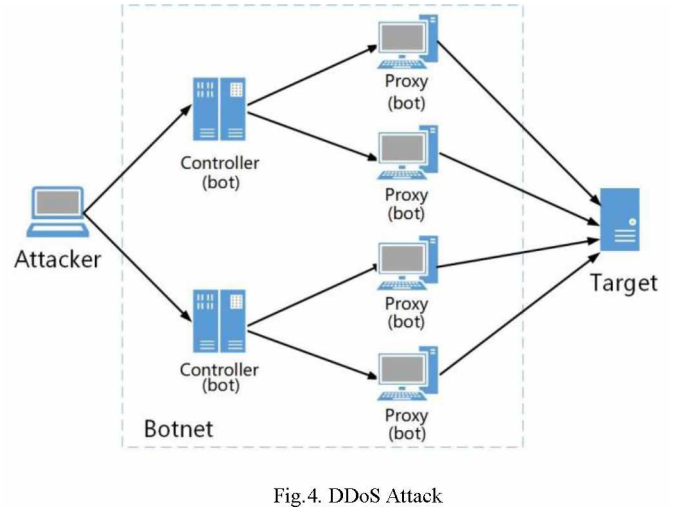

Fig.4. DDoS Attack

Ⅳ. Network Attacks and Traffic Abnormalities

Network Traffic Abnormalities refers that the network traffic deviates from the original level, does not conform to the regular network situation resulting in abnormal situation.

The network anomalies in this paper refer to the anomalies caused by network security problems, such as network attacks. These attacks will send a large number of connection requests in a short time, consume the network resources and bandwidth quickly, artificially with the obvious purpose. It is difficult to predict in advance causing great harm to the network.

One of the common network attacks is DDoS (Distributed Denial of Service)[9], an upgraded version of DoS(Denial of Service), using C/S mode to send a large number of data packets in a distributed and cooperative manner, and consumes the bandwidth and resources as much as possible. In DDoS attacks, many hosts are equipped with some software by attackers. The hosts that are installed these software are called bots, and the network composed of these hosts is called botnet, as shown in Figure 4. After choosing its target, the attacker controls the bots by using the program, at the same time using DoS to attack its target. The dispersion of the numerous hosts not only increases the effect of DoS attack, but also makes it more difficult to find out the source of attack.

Ⅴ. SDN-based IoT Security Architecture Model

A. Model Design

Network security and resource maximum are related to the design of network architecture. The IoT Security Architecture Model combines with SDN technology, effectively improving the security of the IoT and the efficiency of data transmission. The model consists of four layers: perception layer, gateway layer, transport layer and application layer[10], as shown in Figure 5.

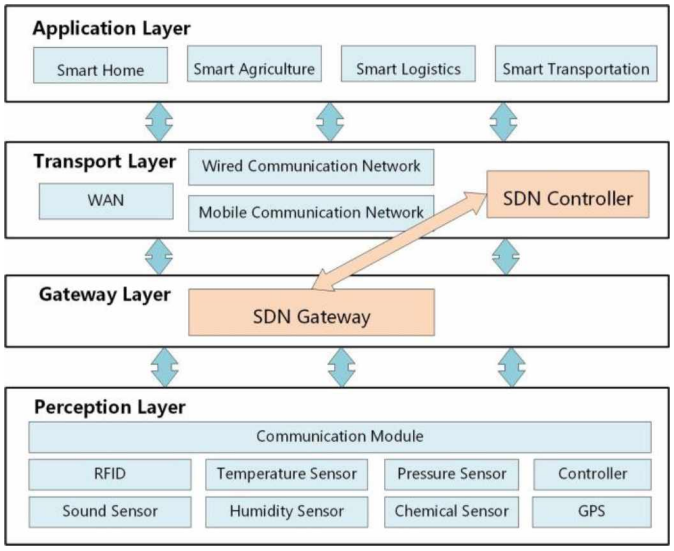

Fig.5. SDN-based IoT Security Architecture Model

Compared with the traditional IoT architecture model, this one adds a gateway layer between the perception layer and the transport layer. Gateway may also be used in traditional IoT architecture model, but only functioning protocol conversion and data packet forwarding.

The gateway layer researched in this paper is the key to integrating SDN technology and IoT. The gateway layer is managed by the controller, and the data packet is analyzed to determine whether to forward to the transport layer. If it is judged that security threat exists, the data will be discarded and not forwarded. In this model, data security checking, classification and decision-making are put forward from the traditional transport layer or application layer to the gateway layer. Through the above processing, only secure data can be forwarded to the transport layer and then to the application layer, which greatly protects the risk of IoT from being threatened, and also reduces the amount of data transmitted in the network. The security policy of the gateway layer can be dynamically configured and adjusted according to the rules measured by the controller.

B. *Security Detection Algorithms*

In this paper, the gateway layer judges the data security through the self-similarity of traffic. Self-similarity is an inherent traffic characteristic of the network itself. Under normal network communication conditions, the global traffic has its self-similarity[11]. But when the network is being attacked, a large amount of data will be exploded in a short time, affecting the self-similarity. Therefore, self-similarity coefficient Hurst can be used to estimate whether the network is being attacked. Hurst is calculated by R/S analytical method. The calculation formula is as follows:

Let $X_i = X_1, \ldots X_n$ be a continuous value of a time series;divide the data into adjacent sub-intervals A; the length of A is H, then A*H=n.

The mean of each sub-interval is:

$$X_m = (X_1 + \cdots + X_h)/H \quad (1)$$

The standard deviation of each sub-interval is:

$$S_h = \sqrt{\sum_{i=1}^{h}(X_i - X_m)^2/h} \quad (2)$$

The cumulative spacing of the mean is:

$$X_{r,A} = \sum_{i=1}^{h}(X_{i,A} - X_m) \quad (3)$$

The intra-group range was as follows:

$$R_h = \max(X_{r,A}) - \min(X_{r,A}) \quad (4)$$

The Hurst is:

$$R_n/S_n = (1/A) \times \sum_{h=1}^{A} R_n/S_n \quad (5)$$

Hurst's relationship is:

$$R_n/S_n = c \times n^H \quad (6)$$

R (n) is extreme deviation; S (n) is standard deviation; n is the number of observed values; C is constant; H is Hurst value. If the Hurst value is between 0.5 and 1, the network traffic has its self-similarity; if the Hurst value is less than 0.5 or more than 1, the self-similarity of network traffic is destroyed.

VI.Simulation Experiments

A. *Experimental Process*

The experiment uses OpenFlow-supported and SDN-based simulation software Mininet [12] to simulate a perception layer and gateway layer including terminals, links and gateways, as shown in Figure 6. After the experimental platform is established, the network traffic under normal conditions is simulated by downloading data, and then the network traffic under DDoS attack is simulated. Specific data packets are captured by software, field values of data packets are extracted, processed and counted. Self-similarity coefficient Hurst values is calculated by R/S analytical method, and can judge whether the network security in this statistical period is satisfactory or not.

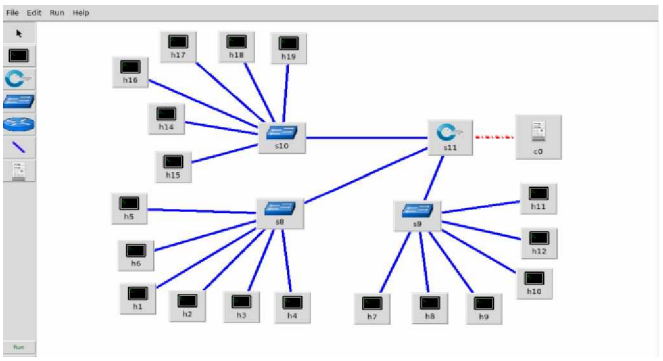

Fig.6. Mininet SDN network topology

B. *Result Analysis*

The Hurst value is calculated by R/S analysis method which is shown in Figure 7. Group 1 to 5 are the Hurst values calculated under normal network traffic conditions, and Group 6 to 8 are the Hurst values obtained under attacks on

the network.

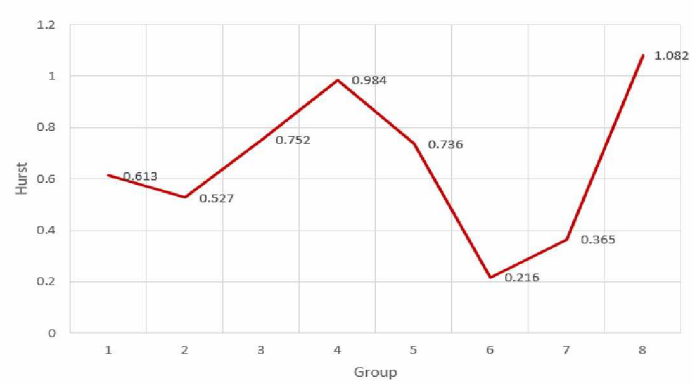

Fig.7. Hurst value calculation result

The experimental results show that when the network traffic is normal, the Hurst value is between 0.5 to 1; when the network is attacked, the Hurst value is less than 0.5 or more than 1. Therefore, the Hurst value reflects the abnormal situation of network traffic and identify the security status of the network.

Ⅶ.Conclusion

By researching the characteristics and security problems of IoT security architecture model, this paper proposes a four-layer IoT architecture model to solve the problem of security of the IoT perception layer. This model applies SDN technology to the IoT, separating logical control and data forwarding in the gateway layer, having the security strategy deployment of the IoT pre-positioned, and making the security rules more flexible and effective. In the specific security strategies, according to the self-similarity of network traffic, the Hurst values can be calculated to effectively detect network traffic anomalies and network attacks. The next step is to test in the real environment, study SDN technology and apply security strategy to the actual Internet of Things system.

REFERENCES

[1] Gubbi J, Buyya R, Marusic S, et al. Internet of Things (IoT): A vision, architectural elements, andfuturedirections[J].Future GenerationComputerSystems,2013, 29: 1645-1660.

[2] H. Huang, J. Zhu and L. Zhang, "An SDN_based management framework for IoT devices," *25th IET Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014)*, Limerick, 2014, pp. 175-179.

[3] McKeownN. Software-definednetworking[J].INFOCOM keynotetalk,2009,17(2): 30-32.

[4] Shin M K,Nam K H, KimH J.Software-defined networking (SDN): A reference architecture and openAPIs[C]//ICTConvergence (ICTC), 2012InternationalConferenceon.IEEE,2012: 360-361.

[5] K. S. Sahoo, B. Sahoo and A. Panda, "A secured SDN framework for IoT," *2015 International Conference on Man and Machine Interfacing (MAMI)*, Bhubaneswar, 2015, pp. 1-4.

[6] Lindstrom P, Villars R L, Marden M. Assessing the Business Value of SDN Datacenter Security Solutions[J]. 2015.

[7] Guo Z, Hu Y, Shou G, et al. An implementation of multi-domain software defined networking[C]//IET Conference Proceedings. The Institution of Engineering & Technology, 2015.

[8] Nick Mc Keown, Tom Anderson, Hari Balakrishnan,etc.. OpenFlow: Enabling Innovation inCampus Networks. ACM SIGCOMM Computer Communication Review，2008.4:69－74

[9] S. S. Bhunia and M. Gurusamy, "Dynamic attack detection and mitigation in IoT using SDN," 2017 27th International Telecommunication Networks and Applications Conference (ITNAC), Melbourne, VIC, 2017, pp. 1-6.

[10] M. T. Kakiz, E. Öztürk and T. Çavdar, "A novel SDN-based IoT architecture for big data," *2017 International Artificial Intelligence and Data Processing Symposium (IDAP)*, Malatya, 2017, pp. 1-5.

[11] Hyukmin Kwon, Taesu Kim, Song Jin Yu, and Huy Kang Kim. Self－similarity Based LightweightIntrusion Detection Method for Cloud Computing. ACIIDS 2011, LNAI 6592, 2011,p 353－362.

[12] Lantz B, O'Connor B. A Mininet-based Virtual Testbed for Distributed SDN Development[J]. Acm Sigcomm Computer Communication Review, 2015, 45(5):365-366.